Využití Knot DNS

v infrastruktuře CZ.NIC

Václav Steiner • vaclav.steiner@nic.cz • 11. 11. 2020

CZ.NIC | SPRÁVCE DOMÉNY CZ

OBSAH

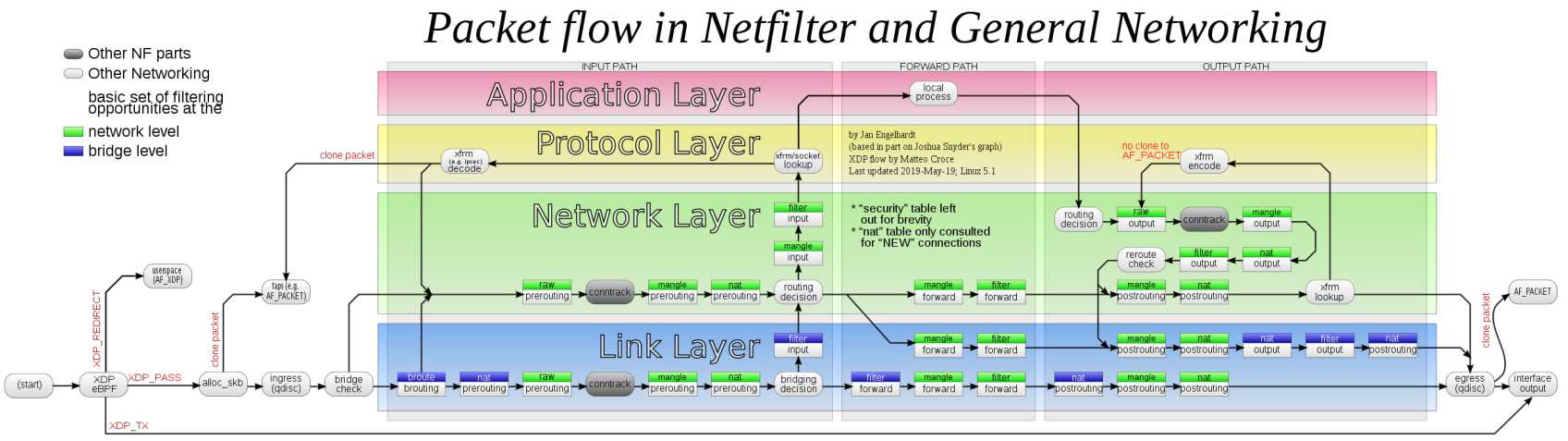
- Knot DNS s využitím XDP
- Knot DNS na HM serverech

KNOT DNS

Knot DNS s využitím XDP

Knot DNS s využitím XDP

- Co je XDP a jaká vylepšení přináší pro DNS provoz?
- Omezení v síťovém stacku



Knot DNS s využitím XDP – konfigurace serverů

- DNS server pro provoz XDP
  - 2x Intel Xeon Gold 6140 18C/36T @ 2,30 GHz (vypnutý HT)
  - 32 GB RAM, SSD disky v RAID1
  - Intel 10GbE X710 SFP+, 2x uplink (LACP), Ubuntu 20.04 LTS
- NET server pro sběr síťového provozu
  - 2x Intel Xeon E5-2695 v3 14C/28T @ 2,30 GHz
  - 64 GB RAM, SAS disky v RAID10
  - Intel 10GbE X710 SFP+, 2x uplink (LACP) Debian 10

Knot DNS s využitím XDP – konfigurace démona

- Nastavit počet front na síťových interfaces

/sbin/ethtool -L ens3f0 combined X

/sbin/ethtool -L ens3f1 combined X

- Nastavit listen v Knot DNS

listen-xdp: ens3f0

listen-xdp: ens3f1

- Rozšířit capabilities v Knot systemd service

CapabilityBoundingSet=CAP_NET_RAW CAP_NET_ADMIN CAP_SYS_ADMIN CAP_SYS_RESOURCE

AmbientCapabilities=CAP_NET_RAW CAP_NET_ADMIN CAP_SYS_ADMIN CAP_SYS_RESOURCE

Knot DNS s využitím XDP – testování výkonu

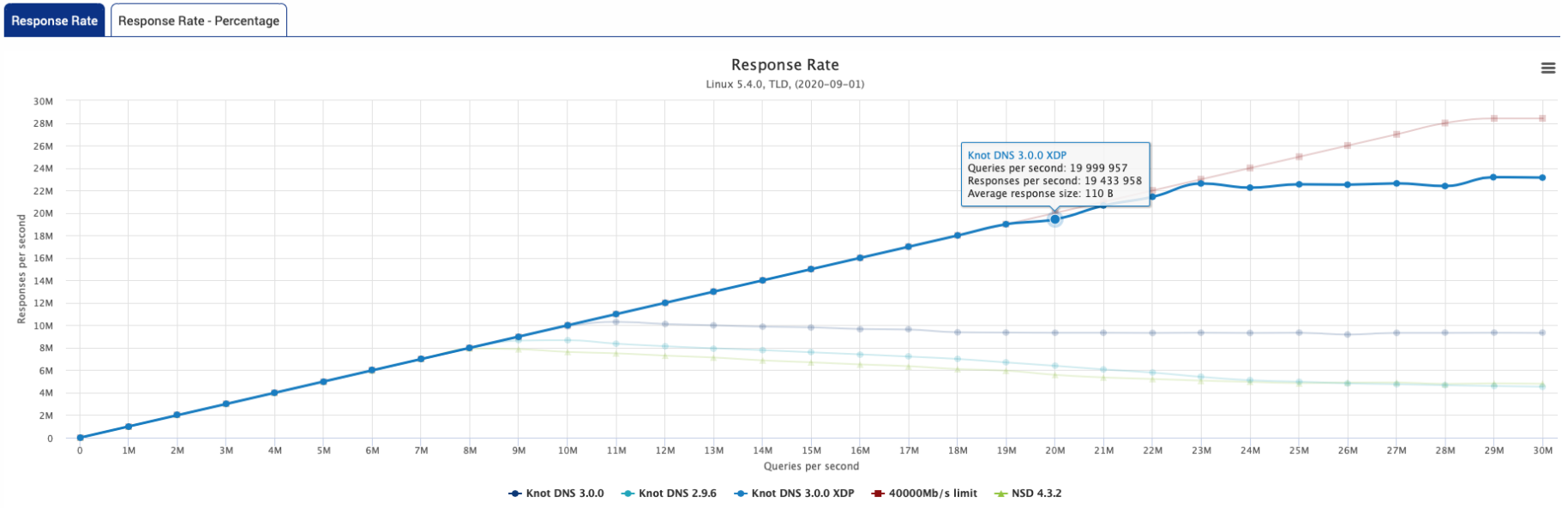
- Nástroj **kxdpgun**
- Tři testovací scénáře
  - DNS dotazy s malými odpověďmi 61B (pozitivní odpovědi bez DNSSEC)
  - DNS dotazy s velkými odpovědmi 788B (negativní odpovědi s DNSSEC)
  - DNS dotazy s odpovědmi o velikost 179B (pozitivní odpovědi s DNSSEC)
- 1x 10GbE linka mezi dvěma servery
- Posláno 10 mio požadavků za sekundu

Knot DNS s využitím XDP – testování výkonu

- Výsledky
  - test č. 1: odbaveno 10 mio QPS, žádná ztrátovost
  - test č. 2: strop 10GbE linky, odbaveno pouze 1,5 – 2 mio QPS
  - test č. 3: odbaveno cca 5 mio QPS

- DNS server bez XDP dokáže při běžném provozu odbavit cca 1 – 1,5 mio QPS.
- S XDP jde tedy o několikanásobný nárůst!

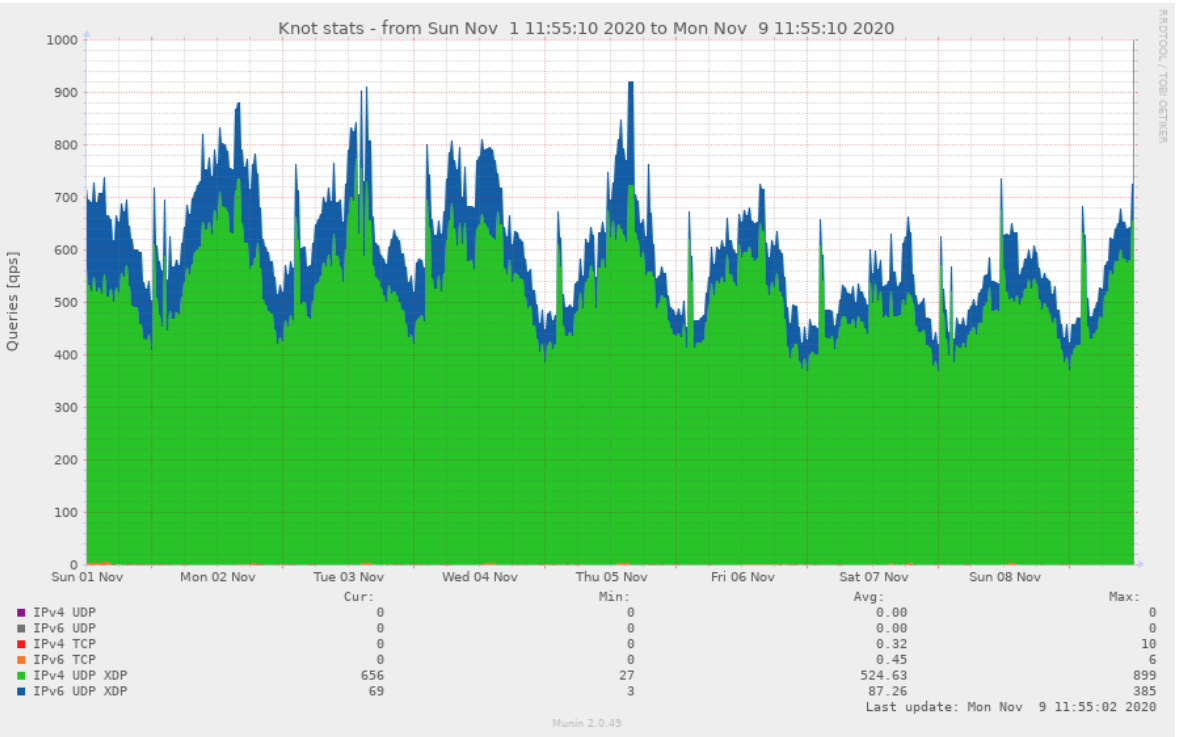
Knot DNS s využitím XDP – benchmark



TLD

- Zones: 1
- DNSSEC: no
- Records: 5182707 total, 1479662 delegations
- Queries: random QNAME, 0% DO
- Replies: 100% NOERROR
- Protocol: IPv4

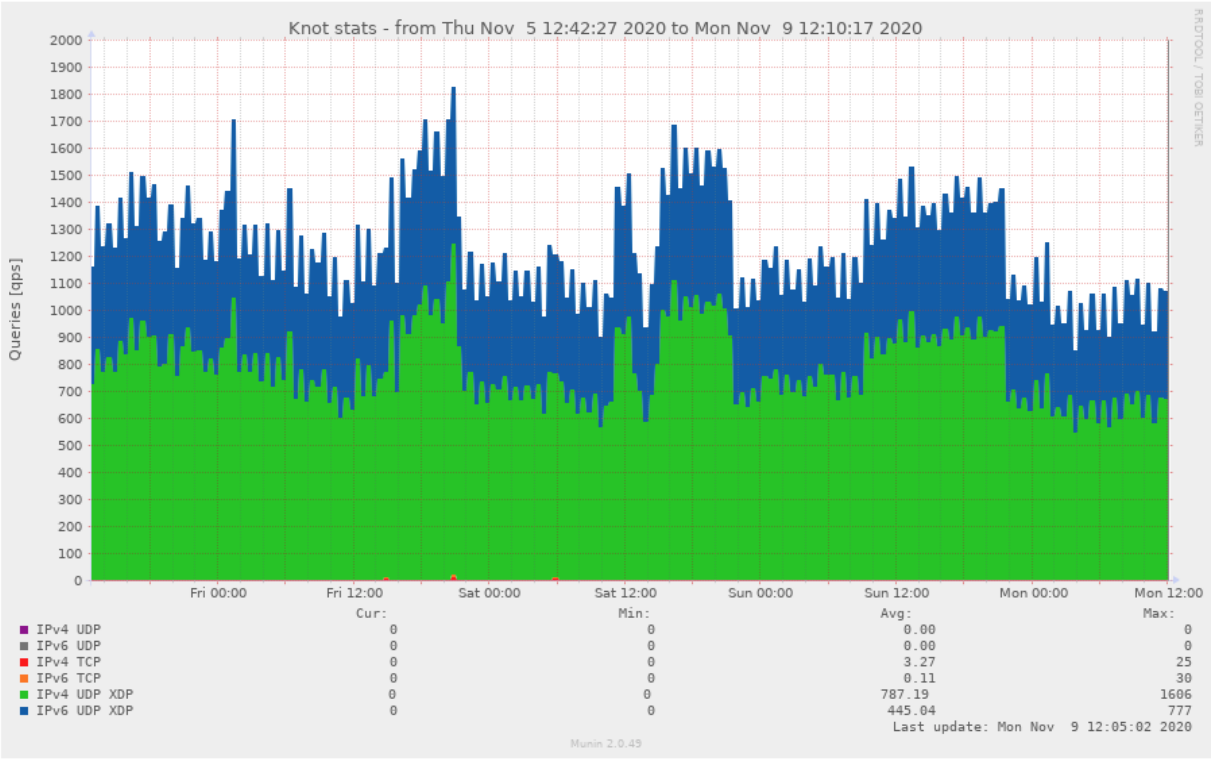
Knot DNS s využitím XDP – statistiky provozu



- Interní Knot DNS statistiky + Munin
  - dns-server> knotc stats
    - UDP4, UDP6
    - TCP4, TCP6
    - UDP4-XDP, UDP6-XDP

Server v ČR mimo 100GbE DNS stacky, použitý anycast **A**

Knot DNS s využitím XDP – nově v Seattle



S XDP to myslíme vážně!

Od 5.11. 2020 nový malý DNS stack v Seattle, WA, USA

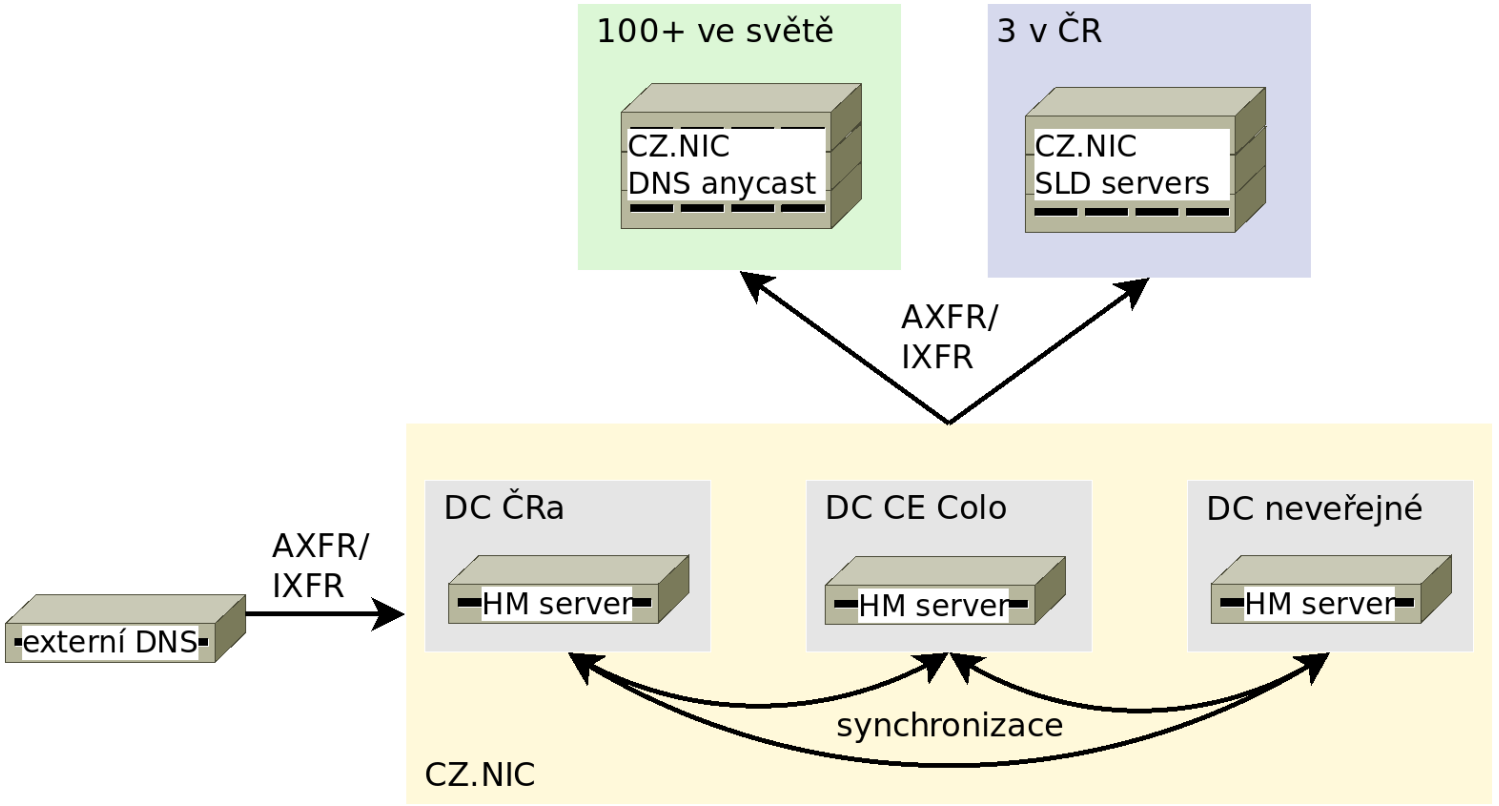
- první s 40GbE
- použitý anycast **A**

Knot DNS na HM serverech

Knot DNS na HM serverech

- Cíle
  - Přechod z BIND
  - Automatické podepisování DNSSEC
    - offline KSK pro ENUM zóna a .CZ
  - Zjednodušení správy a menší chybovost
  - Další rozvoj

Knot DNS na HM serverech - infrastruktura



Knot DNS na HM serverech – původní stav

- Ubuntu LTS, Bind 9.10.x
- ENUM a .CZ zóna z FRED
- vlastní SLD zóny + hosting TLD, SLD
- vlastní scripty pro kontroly zón a podepisování DNSSEC
- cron úlohy

Knot DNS na HM serverech – migrace

- vybudování testovací infrastruktury
- „obětování“ jednoho z HM serverů → Debian 10, KNOT 3.0
- 3. fáze migrace
  - SLD domény na SLD serverech
  - SLD domény na DNS anycastu + hosting TLD, SLD
  - ENUM a .CZ na DNS anycastu
- test přechodu na nepoužívaných doménách – ecdsa.cz, tlsa.cz, gitlab.cz
- nástroje https://dnsviz.net, https://dnssec-analyzer.verisignlabs.com
- 100x otestovaný postup migrace SLD zón + potřebné úpravy DNS serverů (ACL, AXFR/IXFR)
  - import DNSSEC klíčů (KSK společný v .CZ), import zón, úpravy v konfiguracích
  - větší složitost – 3 DNS implementace, postupná migrace po zónách

Knot DNS na HM serverech – migrace

- test přechodu na méně používaných doménách – agresivnihrypronejmensi.cz, strejduvskvelymed.cz, …
- CDNSKEY pro zvěřejňování klíčů do .CZ
- PTR DNS anycastu, mojeid.cz a nic.cz až nakonec
- hosting SLD a TLD zón vlastně nejjednodušší (pouze „relay“)
- .CZ a ENUM zóny komplikovanější postup – offline KSK
  - příprava nového podepisovacího řešení pro CSIRT

Knot DNS na HM serverech – migrace v číslech

- CZ.NIC: 123 zón + 32 PTR
- Hosting TLD, SLD: 66 zón + 18 PTR
- fáze č. 1 a č. 2 dokončena na konci října 2020

- První SLD zóny už mají provedenou KSK rotaci
- ENUM v následujících dnech, .CZ do konce listopadu 2020

Knot DNS na HM serverech – přínosy

- zjednodušená správa zón
- nemusíme se starat o podepisování (vyjma .CZ)
- žádné vlastní scripty a cron úlohy
- menší náchylnost na chyby
- změny v SLD zónách jsou okamžité
- možnosti do budoucna – inkrementální změny v .CZ, rychlejší generování a publikace .CZ zóny ...

„Přijďte“ do Akademie

- Chystáme praktický kurz na použití Knot DNS s automatickým podepisováním DNSSEC
- 2021Q1, bude zveřejněn
- https://akademie.nic.cz

Děkuji za pozornost

Václav Steiner • vaclav.steiner@nic.cz

CZ.NIC | SPRÁVCE DOMÉNY CZ

Zdroje

- https://en.wikipedia.org/wiki/Express_Data_Path
- https://blog.nic.cz
- https://pixabay.com/vectors/checklist-lists-business-form-41335/
- https://pixabay.com/vectors/cowboy-gun-guns-outlaw-retro-2028626/
- https://www.knot-dns.cz/benchmark/
- https://akademie.nic.cz